Wireless Campus: un Esempio di Trasferimento Tecnologico Applicato a Tecnologie Wireless

Andrea Ghittino, Davide Ferri, Elisa Marchioro, Oronzo Giulio Petito
Dipartimento Tecnologie, CSP Innovazione nelle ICT, Torino (Italia)
andrea.ghittino@csp.it, elisa.marchioro@csp.it, davide.ferri@csp.it, oronzo.petito@csp.it

Abstract: il progetto Wireless Campus nasce dall'esperienza di CSP nello studio e nell'analisi di scenari di ICT evoluti e dall'intento di Environment Park di adeguare il parco tecnologico torinese con sistemi telematici all'avanguardia.
Il punto di partenza del progetto sono state le WLAN, ad oggi uno degli argomenti di maggior interesse nel panorama delle soluzioni al problema della mobilità degli utenti.
I principali obbiettivi del progetto sono due: da un lato un servizio sperimentale di connettività wireless e dall'altro un laboratorio di test e analisi di scenari e soluzioni high-tech nell'ambito delle reti wireless LAN.
Dopo una prima fase dedicata alla creazione di un'infrastruttura di rete WLAN ed alla possibilità di connettersi in rete in modo sicuro, l'attenzione del progetto sarà concentrata sui servizi e sulla loro migrazione in ambiente wireless; in particolare si analizzerà l'introduzione di servizi innovativi quali streaming, telefonia su IP, videoconferenza e servizi basati sulla localizzazione degli utenti (LBS).

Panoramica sulla tecnologia

Prima di esaminare in dettaglio il progetto Wireless Campus, è necessario soffermarsi sulla principali caratteristiche delle tecnologie wireless impiegate nel progetto e sulle metodologie da applicare per garantire al sistema un adeguato livello di sicurezza.

Le WLAN 802.11

Wireless LAN (o WLAN) è il termine con cui si indica una tipologia di rete in cui il mezzo trasmissivo è rappresentato dal canale radio.
In ambito di wireless LAN sono disponibili diverse tecnologie di rete, fra le quali spiccano le reti conformi allo standard IEEE 802.11b, attualmente le più diffuse sia perché funzionanti in una banda di frequenze non soggetta ad assegnazione esclusiva (ISM, Industrial Scientific Medical) sia per l'accessibilità economica delle apparecchiature e la (apparente) semplicità di configurazione.
Lo standard 802.11 nasce nel 1997, e definisce le caratteristiche di un protocollo di livello MAC (Medium Access Control) che consente il trasporto dei pacchetti IP sul canale radio. La banda di frequenze è definita fra 2.402 e 2.482 GHz, per un totale di 13 canali (secondo la normativa ETSI valida per l'Europa), a ciascuno dei quali corrisponde una portante radio, modulata in FHSS o DSSS.
Nel corso degli anni, lo standard di partenza si è arricchito di alcune varianti, definite per venire incontro a requisiti di servizi della tecnologia stessa che si andavano delineando in seguito alla sua progressiva diffusione. Alcuni aspetti sono già stati ratificati come addendum agli standard principali (802.11a e 802.11b), mentre altri sono ancora in forma di draft e riguardano gli argomenti ancora in fase di studio e approfondimento, verso cui punta la ricerca scientifica.

Il Sistema di Trasmissione

Il "mezzo trasmissivo aria" è una risorsa condivisa tra tutte le stazioni wireless e gli access point. Tra tutti gli apparati 802.11 che utilizzano un determinato canale radio ce ne può essere solo uno attivo. Se più entità trasmettono contemporaneamente, si verifica una collisione e tutti i pacchetti coinvolti risultano corrottti ed è quindi necessario ritrasmetterli.
Le reti cablate (Ethernet, ad esempio) sono progettate in modo che tutte le stazioni siano in grado di rilevare un'eventuale collisione; al contrario, in ambiente wireless non c'è garanzia che tutte le stazioni la rilevino. La disposizione delle stazioni all'interno di una WLAN non è prefissata: avvicinandosi alla rete si riceve il segnale delle stazioni più vicine mentre quelle più lontane possono non essere rilevate; questa situazione crea delle ambiguità.
Al fine di rilevare se una trasmissione è andata a buon fine o meno, viene utilizzato un sistema di ritrasmissione dei frame con conferma attraverso pacchetti di ack.
Per ottimizzare le performance del sistema è stato adottato un protocollo per ridurre al minimo le collisioni, detto Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA). Esso utilizza due messaggi: "Request To Send" (RTS) e "Clear To Send" (CTS) per assicurare agli utenti un intervallo di tempo libero in cui trasmettere i propri dati.
L'inconveniente dell'uso di RTS e CTS è un overload di traffico, che per frame dati di piccole dimensioni può essere significativo; al contrario, se il sistema RTS/CTS è attivo le collisioni si possono verificare solo durante la fase di RTS. Di solito il frame RTS è molto più corto di un frame dati ed il tempo perso a causa delle collisioni è ridotto: in questo modo, le prestazioni complessive del sistema risultano più elevate.
Le topologie di rete wireless possono essere distinte in: peer-to-peer, nel qual caso i client wireless comunicano direttamente fra loro, oppure basate su access point, intermediari fra end-point e backbone (cablato o wireless). Quest'ultimo è il caso più frequente, per favorire l'integrazione del sistema WLAN con la rete locale cablata.

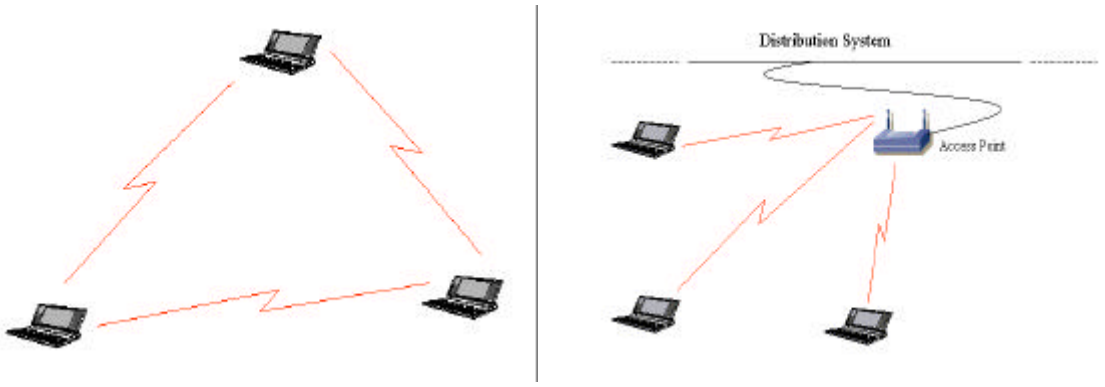

Figura 1: Architettura di una rete WLAN: ad hoc (a sinistra) e come infrastruttura

A livello architetturale superiore si trovano WLAN dotate di access point con funzioni di bridging punto-punto oppure punto-multipunto, in base alla capacità di collegare fra loro una o più WLAN dislocate in edifici distanti tra loro anche alcuni km. Si attivano allo scopo collegamenti diretti in radiofrequenza, in situazioni di campo libero da ostacoli (edifici, alberi, ecc.), con caratteristiche diverse a seconda del tipo di antenne impiegate e delle condizioni ambientali.

Elementi di Sicurezza

Le problematiche inerenti la sicurezza in reti wireless lan sono legate all'accesso al canale radio da parte di utenti non autorizzati, che possono portare ad:

- Accesso non autorizzato alle risorse del sistema;

- Intercettazione del segnale trasmesso sulla WLAN (eavesdropping).

Per migliorare la sicurezza del sistema lo standard 802.11b introduce due meccanismi di protezione:

- Service Set ID (SSID) – identificativo per l'accesso alla WLAN da parte dei client wireless
- Wired Equivalent Privacy (WEP) – sistema che comprende meccanismi di autenticazione degli utenti e cifratura delle comunicazioni

Sono in via di standardizzazione ulteriori specifiche relative alla sicurezza, definite dall' IEEE Security Subgroup 802.11i, finalizzate al perfezionamento degli algoritmi di cifratura per reti 802.11.
I problemi legati alla sicurezza hanno rappresentato uno dei maggiori ostacoli alla diffusione delle WLAN. Ad oggi sono state identificate diverse fonti di vulnerabilità, soprattutto correlate alle specifiche per la sicurezza del protocollo inserite nello standard 802.11. In particolare, studi accreditati hanno dimostrato come sia possibile eseguire una serie di attacchi specifici ad una rete WLAN 802.11 per violare le trasmissioni di altri utenti oppure utilizzare la rete d'accesso in modo fraudolento. Gli stessi studi, tuttavia, hanno rappresentato una base di partenza per procedere verso il progressivo miglioramento degli strumenti di difesa contro gli attacchi alla rete: ad esempio, lo stesso protocollo WEP per l'autenticazione e la cifratura delle trasmissioni si basa sull'impiego di chiavi di sessione più o meno deboli a seconda del particolare vettore di inizializzazione utilizzato per generarle, per questo motivo, scegliere di implementare vettori che diano luogo a chiavi "forti" rappresenta di per se una miglioria rispetto alle condizioni originarie di funzionamento del sistema.

802.1x

L'IEEE sta studiando un nuovo standard (802.1x) da utilizzare per massimizzare la sicurezza delle reti wireless e centralizzare le funzioni di gestione della rete. Come parte delle proposte vi è l'EAP (Extensible Authentication Protocol) che permette ai client wireless di autenticarsi con dei server RADIUS utilizzando il metodo del sign-on.
In questa modalità il RADIUS assegna ai client wireless delle chiavi WEP dinamiche per la sessione in corso. Tutti i dati sono crittografati utilizzando l'algoritmo RC4 con chiavi a 128 bit, prevenendo così gli attacchi di tipo man-in-the-middle, monitoring passivo e attacchi simili. Inoltre le chiavi cambiano con una frequenza tale che un eventuale attaccante non è in grado di accumulare abbastanza dati per effettuare il "cracking" della chiave.
Con l'autenticazione di tipo 802.1x, il client si associa ad un AP normalmente, ma l'AP blocca l'accesso alla rete cablata durante la fase di autenticazione. L'AP inizia il protocollo EAP con il client, quindi trasmette le comunicazioni tra il client ed uno speciale RADIUS server EAP abilitato sulla rete wired. Una volta che le credenziali del client sono state stabilite, il RADIUS server impone le politiche di accesso all'AP. A questo punto, l'AP da al client l'accesso alla rete wired, con le appropriate restrizioni. Come parte di questo processo, l'AP assegna dinamicamente una chiave al client, la trasmissione di questa è effettuata usando una separata chiave che è generata dal RADIUS server e passata all'AP.
In una rete in cui ogni client ha una propria chiave distinta diventa enormemente più arduo ottenere sufficienti dati per realizzare attacchi mirati.

Wireless Campus

Dopo una rapida panoramica sulle principali tecnologie utilizzate nel corso del progetto si può iniziare ad esaminare gli aspetti salienti della realizzazione dell'infrastruttura wireless.

La Filosofia del Progetto

CSP ed Environment Park nell'avviare il progetto Wireless Campus si sono posti come obiettivo principale quello di creare un *test-bed* per poter sperimentare i servizi wireless nelle normali attività di tutti i giorni.
Il primo passo per Wireless Campus è la progettazione e la realizzazione dell'infrastruttura di rete 802.11b; il secondo passo riguarda, invece, i servizi, che risultano innovativi rispetto a quelli di semplice navigazione su rete Internet e consultazione della posta elettronica. Inoltre, il modello adottato per il

trasferimento tecnologico delle competenze e dei risultati della sperimentazione andranno a beneficio di una rete sperimentale sulla quale Environment Park acquisisce i servizi in veste prototipale e CSP riceve un feedback da parte degli utenti di test sulla fruibilità del sistema.
In particolare, il CSP propone le WLAN come argomento di studio e ricerca su cui fornire feed-back a livello scientifico e prototipare servizi ed applicazioni.

Dal punto di vista tecnico, l'idea di partenza è stata quella di costruire una vetrina all'interno della quale introdurre di volta in volta dispositivi di produttori diversi (e, ove disponibili, opensource),al fine di verificarne le diverse caratteristiche e, soprattutto, l'interoperabilità. Per raggiungere questo obiettivo, sono state definite una serie di *building block* ben distinti; tra questi i principali sono il sistema di autenticazione, il backbone della rete e la rete di accesso.
Il risultato complessivo è una rete in grado di evolvere continuamente, integrando nuovi dispositivi e nuovi servizi, in modo trasparente per l'utente finale.

Un ultimo aspetto riguarda l'utilizzo di soluzioni opensource: CSP ed Environment Park ritengono di primaria importanza utilizzare all'interno di Wireless Campus sistemi opensource sia per confrontarli con le equivalenti soluzioni commerciali sia per potere intervenire sui singoli componenti per ottimizzarne le prestazioni. Attualmente, si stanno sperimentando:

- l'access point opensource "HostAP";
- il server RADIUS "FreeRadius".

In particolare, le attività relative all'access point opensource hanno come obiettivo di ottimizzare la gestione della qualità del servizio per le applicazioni multimediali.

Realizzazione del Progetto

L'infrastruttura di rete viene realizzata attraverso diverse fasi:

- la prima ha lo scopo di individuare le aree ottimali all'interno delle quali attivare gli access point: sono state individuate alcune aziende "campione" all'interno del Parco tecnologico ed alcune aree comuni (ad esempio sale riunioni) al cui interno offrire una copertura 802.11b;
- la seconda fase vede la realizzazione di test e verifiche sul campo al fine di ottimizzare il posizionamento degli access point per garantire una copertura radioelettrica il più uniforme possibile;
- la terza fase del progetto prevede l'estensione della copertura di rete wireless, integrando ulteriori access point in modo da collegare tra loro le "isole" wireless create nella prima fase;

In seguito alla realizzazione dell'infrastruttura, saranno attivati i servizi sperimentali. Il modello di attivazione è il seguente:

- Si parte dall'attività sperimentale per definire completamente i requisiti tecnici necessari alla realizzazione del particolare tipo di servizio;
- Si passa poi allo sviluppo di un prototipo del servizio, che verrà sottoposto in seguito a test e verifiche sulle potenzialità del servizio stesso e per definire i requisiti di attivazione (configurazione server, terminali, rete fissa, WLAN, ecc.).

Al termine di un periodo di prova sulla rete Wireless Campus, il feedback degli utenti di prova sarà utilizzato per valutare la bontà e l'efficacia del servizio stesso.

I Servizi

Il progetto consente di realizzare un ambiente di studio in cui si possono verificare diversi scenari di servizio, di cui viene data qui una breve panoramica.

Connettivià di Rete

Il primo obiettivo di Wireless Campus è quello di consentire agli utenti presenti in Environment Park di essere "on-line" anche al di fuori del proprio ufficio, continuando ad accedere ai servizi ed alle proprie infrastrutture sempre con le stesse modalità.
Rispetto all'interconnessione con altri enti, invece, la rete Wireless Campus funziona come uno degli hot-spot interconnessi fra loro attraverso un backbone di rete fissa. Per questo motivo si ipotizza una futura espansione della rete sulla quale implementare sistemi di autenticazione centralizzati attraverso un unico server radius e condivisi poi dai vari elementi del sistema di hot-spot.
In questo caso ciascun utente sarebbe in grado di spostarsi da un hot-spot all'altro mantenendo la possibilità di collegarsi alla rete nelle diverse località.

Multimedia e Wireless

L'implementazione di servizi multimediali su rete wireless LAN rappresenta un argomento di grande intresse: se da un lato questi servizi apportano notevoli vantaggi per l'utente finale quando questo si sposta con un terminale mobile, dall'altro si pongono alcune problematiche per trasportare i servizi stessi sulla rete wireless LAN.
Fra i possibili servizi multimediali, sono compresi quelli di comunicazioni telefoniche (VoIP), videoconferenza e streaming di contenuti multimediali. I primi due sono servizi real-time, ovvero sensibili ai ritardi introdotti dalla rete, ma soprattutto alla variabilità delle condizioni della rete, che determinano un degrado della qualità, soprattutto a livello audio, percepita dall'utente finale.
Per garantire un adeguato livello di servizio, è necessario, in primo luogo pianificare correttamente l'integrazione dei server nell'architettura, ma anche e soprattutto intervenire sulla rete wireless per attivare politiche di qualità del servizio che diano priorità al traffico multimediale rispetto a quello dati.

Servizi di Localizzazione

I servizi di localizzazione (LBS) hanno un ruolo importante nella realizzazione di servizi destinati all'utenza mobile, come valore aggiunto rispetto ai servizi primari di connettività di rete.
Lo strumento ad oggi più diffuso per i servizi di localizzazione è il ricevitore GPS: il costo relativamente contenuto e la possibilità di utilizzarlo in abbinamento o integrato in oggetti di largo consumo (cellulari, optional per automobili, orologi, ecc.) ne hanno favorito la diffusione.
Per applicazioni indoor esistono diverse tecniche di rilevamento della posizione, fra le quali stanno emergendo le tecnologie legate a sistemici rete wireless LAN, in particolare l'802.11.
L'attenzione verso questi sistemi è dovuta alle loro caratteristiche intrinseche: ciascun client di rete effettua misure sul livello del segnale radioelettrico ricevuto come parte del sistema di connessione alla rete, quindi non è essenziali avere a disposizione dispositivi aggiuntivi.

Always on-line: WLAN e GPRS

Un altro aspetto di interesse riguarda la possibilità di utilizzare il sistema GPRS come alternativa al sistema WLAN per l'accesso ad Internet e la consultazione della posta elettronica in località esterne rispetto all'area di copertura del parco.
Oltre ai questi servizi, Wireless Campus si pone come obiettivo di consentire agli utenti di continuare a "comunicare" con i propri colleghi anche al di fuori della copertura 802.11b; a tal fine, si stanno sperimentando soluzioni basate sul protocollo SIP che uniscono alla gestione di voce e video anche servizi di "presenza" (per verificare in ogni momento quali sono i propri colleghi presenti in rete) e di "instant messaging". In questo modo, anche all'interno della rete GPRS gli utenti possono interagire tramite messaggi testuali sfruttando la stessa infrastruttura (e quindi gli stessi identificativi degli utenti, lo stesso sistema di autenticazione, …) utilizzati per la telefonia su IP.

Dal punto di vista pratico, i terminali sono provvisti di schede che presentano uno slot interno per alloggiare una scheda SIM per servizi di telefonia cellulare: inserendo la propria scheda abilitata al

servizio, è possibile connettersi ad Internet con il portatile o il proprio dispositivo palmare, utilizzando la stessa scheda che permette di collegarsi alla WLAN del parco.
In un'ottica sperimentale più ampia, il CSP collabora con uno degli operatori nazionali di telefonia cellulare per la sperimentazione di servizi di connettività.

La Gestione della Rete: il Trasferimento Tecnologico

CSP è impegnato nella ricerca e sperimentazione su sistemi wireless lan, in collaborazione con il Politecnico di Torino. Dallo studio e analisi delle caratteristiche tecnologiche dei sistemi wireless LAN nascono proposte di sviluppo di nuovi servizi di rete, in cui è stato coinvolto Environment Park, quale azienda attiva sulla fornitura di servizi ICT innovativi internamente al parco tecnologico.
Attraverso il progetto Wireless Campus, il CSP si è impegnato sul piano tecnico per realizzare una rete wireless LAN che potesse estendere anche ad Environment Park l'adozione delle nuove tecnologie di rete mobile e nel contempo lavorare su di un caso concreto di rete WLAN estesa.

Le linee guida per il trasferimento tecnologico sono le seguenti:

- in primo luogo CSP, identifica una tecnologia od un servizio tra quelli analizzati all'interno dei laboratori e al Politecnico di Torino come maturo per essere sperimentato su un numero ristretto di utenti;
- dopo un periodo di prova, si verifica il feed-back ricevuto sia sulle caratteristiche del servizio sia sulla sua effettiva utilità; gli amministratori di Wireless Campus, inoltre, utilizzano questo periodo per verificare l'impatto sulla rete e sui servizi già presenti;
- il terzo passo prevede di estendere il servizio a tutti gli utenti, sempre con particolare attenzione all'impatto sulla rete e al feed-back degli utenti. In questa fase, in genere, si interviene sul servizio introducendo piccole ottimizzazioni, mentre le variazioni più significative richieste dagli utenti vengono riportate ai laboratori di CSP;
- infine, una volta completata anche la terza fase, CSP cura il passaggio di competenze ed assiste il nuovo amministratore nella prima fase della sua gestione.

In questo modo, quando dall'attività di ricerca di CSP e Politecnico scaturisce lo stimolo a promuovere nuovi servizi per reti wireless, questi vengono sviluppati in forma prototipale dal CSP. Dopo essere stati sottoposti ad una serie di verifiche sul campo, i servizi passano alla fase di produzione e vengono dati in gestione al parco, insieme alle competenze necessarie a completare il trasferimento tecnologico.

References:

[1] D. Gibbon, R. Moore, R. Winski Eds., *Handbook of Standards and Resources for Spoken Language Systems*. Volume IV: Spoken Language Reference Materials, Mouton de Gruyter, 1998.

[2] Seybert A.F., Ross D.F., Experimental determination of acoustic properties using a two microphone random excitation technique, J. Acoustic Soc. Am. Vol. 61, 1977, 1362-1370.